UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

KENNETH HASSON, on behalf of himself and all others similarly situated, Plaintiff, v. SAMSUNG ELECTRONICS AMERICA, INC., Defendant.	Case No.: 2:22-Cv-1669 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kenneth Hasson ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated (the "Class") against Defendant Samsung Electronics America, Inc. ("Samsung" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action against Samsung for Samsung's failure to properly secure and safeguard protected personally identifiable information, including without limitation, first and last name, demographic information, date of birth, and product registration information (collectively, "PII"), for failing to comply with industry standards to protect information systems that contain PII, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised. Plaintiff seeks, among other things, damages, orders requiring Samsung to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably adequate security practices and safeguards to prevent incidents like the disclosure in the future, and for Samsung to

provide identity theft protective services to Plaintiff and Class Members for their lifetimes, as Plaintiff and Class Members will be at an increased risk of identity theft due to the conduct of Samsung described herein.

2. Samsung is a technology and electronics company that sells millions of products per year with revenue of approximately $244 billion.[1] Samsung is one of the of the largest technology companies in the world serving hundreds of millions of electronic device owners and users.[2]

3. While Samsung purports to protect its customers' personal data with industry leading security protections, on September 2, 2022, Samsung announced that malicious hackers had breached Samsung's systems and made off with its customers' valuable PII (the "Data Breach").[3]

4. Samsung's poorly explained Data Breach notice, coupled with its unexplained delay in disclosing the Data Breach has left its customers without a clear idea of the scope of the Data Breach, the extent of the information affected, and what they need to do to protect themselves.

5. As a result of Samsung's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of cyber-criminals. Plaintiff and Class Members face a substantial increased risk of identity theft, both currently and for the indefinite future. Consequently, Plaintiff and Class Members have had to spend, and will

---

[1] Federica Laricchia, *Samsung Electronics – Statistics and Facts*, Statista (Apr. 5, 2022), https://www.statista.com/topics/985/samsung-electronics/#topicHeader__wrapper.

[2] Zach Whittaker, *Parsing Samsung's Data Breach Notice*, TechCrunch (Sept. 6, 2022), https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice/.

[3] *Important Notice Regarding Customer Information*, Samsung (Sept. 2, 2022) ("Data Breach Notice"), https://www.samsung.com/us/support/securityresponsecenter/.

continue to spend, significant time and money to protect themselves due to Samsung's security failures.

6. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, negligence *per se*, unjust enrichment, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the of adoption reasonably adequate security practices to safeguard the PII in Samsung's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

7. Plaintiff Kenneth Hasson is a citizen and resident of the Commonwealth of Pennsylvania.

8. Plaintiff Hasson owns a Samsung smartphone and Samsung Smart TV. For use with his Samsung devices, Plaintiff Hasson created a Samsung Account, providing Samsung with PII, including his name, address, email address, date of birth, phone number, and other information. When creating his Samsung Account and entrusting his PII to Samsung, Plaintiff reasonably expected that Samsung would take reasonable steps to safeguard his PII.

9. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII – time which he would not have had to expend but for the Data Breach.

10. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages, for years to come.

11. Defendant Samsung Electronics America, Inc., is a New York corporation with a principal place of business located at 85 Challenger Road, Ridgefield, New Jersey 07660-2118. Defendant is a citizen of New York.

12. Defendant is a wholly owned subsidiary of Samsung Electronics Co., Ltd, a South Korean based corporation whose principal place of businesses is located in the Republic of Korea. Defendant is responsible for the production and sale of electronics sold in the United States.

JURISDICTION

13. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 Members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

14. The Court has personal jurisdiction over Defendant because Defendant transacts substantial business in this District, has substantial aggregate contacts with this District, and purposefully availed itself of the laws of Pennsylvania in this District, because the acts and transactions giving rise to this action occurred in this District.

15. Pursuant to 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the events, omissions, and acts giving rise to Plaintiff's claims herein occurred in this District.

FACTUAL BACKGROUND

16. Samsung is a global market leader in high-end electronics manufacturing. Its products include electronics such as Galaxy phones, Galaxy tablets, smart watches, televisions, appliances, computer monitors, and more.[4]

17. Samsung offers purchasers of its products a "Samsung Account" which is an integrated membership that allows Samsung users to enjoy all Samsung's exclusive services on their smartphones, tablets, websites, televisions, and other Samsung products.[5] Such exclusive services include but are not limited to, the Galaxy Store, Samsung Pay, Samsung Rewards, and Samsung Health.[6]

18. Plaintiff, like millions of other Samsung users, created a Samsung Account and entrusted Samsung with personal information in order to receive the exclusive benefits of a Samsung Account.

19. When a customer creates a Samsung Account, the customer may provide Samsung with PII that includes contact information including name, email address, postal address, and phone number; payment card information; date of birth; gender; information stored in or associated with the Samsung Account (including Samsung Account profile, ID, username,

[4] *See* Samsung, https://www.samsung.com/us/ (last visited Nov. 17, 2022).

[5] *Samsung Account*, Samsung, https://order-help.us.samsung.com/hc/en-us/articles/4416742944403-What-is-a-Samsung-account-and-how-do-I-create-one- (last visited Nov. 17, 2022).

[6] *One Account. Everything Samsung.*, Samsung, https://www.samsung.com/us/samsung-account-benefits/ (last visited Nov. 17, 2022).

and password); the username and password for participating third party devices, apps, features, and services; and more.[7]

20. In turn, Samsung uses the PII that Plaintiff and other consumers entrusted to it to provide and enhance Samsung services; provide targeted ads to Samsung users; communicate with Samsung users; provide customer support; and "operate, evaluate, and improve" its own business by "developing new products and services," "conducting market research," and, "performing data analytics."[8] Samsung even purports to collect large amounts of personal data from its device users to "protect against, identity, and prevent fraud and other criminal activity."[9]

21. Understanding how "important privacy is to [its] customers,"[10] Samsung asserts it "take[s] data security very seriously."[11] Samsung "products are designed to keep [] data private and secure while always pushing forward to offer [] the latest, most groundbreaking innovation."[12] Indeed, according to Samsung, security is "in [its] DNA" and "no matter what's ahead, [Samsung] will be ready to protect [consumers] in the digital world."[13]

22. However, despite Samsung's representations that it has spent years perfecting its security platform, and that Samsung "users can have peace in mind with Samsung's industry-

---

[7] *Samsung Privacy Policy for the U.S.*, Samsung (last updated Oct. 1, 2022), https://www.samsung.com/us/account/privacy-policy/.

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Samsung's Privacy Principles*, Samsung, https://www.samsung.com/us/privacy/ (last visited Nov. 17, 2022).

[12] *Id.*

[13] *Secured by Knox*, Samsung, https://www.samsung.com/us/security/ (last visited Nov. 17, 2022).

leading security,"[14] Samsung's promises fell flat when it failed to safeguard Plaintiff's and Class Members' PII from being exfiltrated by cyber-criminals, failed to inform Plaintiff and Class members for weeks that their PII had been compromised, and left consumers without any clear idea of the extent of the PII compromised in the Data Breach, or how to protect themselves.

A. The Value of Private Information and Effects of Unauthorized Disclosure.

23. As electronic device giant who prides itself on being an industry leader in data security, Samsung was well aware that the protected PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

24. "Personal Data is currency in the Information Age and is being traded to the tune of billions of dollars globally – and increasing each year as the more personal data is analysed [sic], categorised [sic] and linked."[15]

25. PII carries immense value to not only companies and social media platforms, but to cyber criminals as well who seek to steal PII for a variety of reasons including blackmail, identity theft, extortion, and sale on underground internet websites, commonly referred to as the "dark web."[16]

---

[14] *Welcome to Samsung Mobile Security*, Samsung, https://security.samsungmobile.com/main.smsb (last visited Nov. 17, 2022).

[15] *The Value of Personal and Private Data*, Digital Control Room, https://www.digitalcontrolroom.com/the-value-of-personal-and-private-data/ (last visited Nov. 17, 2022).

[16] *How Much is Your Data Worth? The Complete Breakdown for* 2021, Invisibly (Jul. 13, 2021), https://www.invisibly.com/learn-blog/how-much-is-data-worth/.

26. Indeed, cybercriminals can use stolen PII to target individuals with phishing and other social engineering attacks and to distribute malware,[17] especially since the breadth of the PII compromised in the Data Breach reveals to cyber-criminals a detailed picture about a Samsung user and their online habits.

27. The ramifications of Samsung's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

28. Further, cyber-criminals often trade stolen PII on the "cyber black market" for years following a breach. Cyber-criminals can also post stolen PII on the internet, thereby making such information publicly available.

29. Samsung knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. Samsung failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring, resulting in the theft of PII Plaintiff and Class Members entrusted to Samsung.

B. Samsung Demonstrates a Reckless Disregard For Data Security.

30. Samsung has an obligation to securely maintain the customer PII that it receives and keep it safe from harm. Samsung knows that PII, specifically when it includes detailed information collected from Samsung device users, is a prime target for cyber-criminals. Indeed, despite claiming to be an industry leader in data security, Samsung has been twice breached by cyber-criminals this year.

[17] Ravi Sen, *Here's How Much Your Personal Information is Worth to Cybercriminals – and What They Do With It*, PBS (May 14, 2021), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.

31. In March 2022, Samsung confirmed that cyber-criminals obtained and leaked almost 200 gigabytes of confidential data, including source code for various technologies and algorithms for biometric unlock systems.[18]

32. The Lapsus$ hacking group claimed responsibility for the March 2022 data breach, asserting that it "obtained source code for trusted applets installed in Samsung's TrustZone environment, which Samsung phones use for performing sensitive operations, algorithms for all biometric unlock operations and bootloader source code for all recent Samsung Galaxy devices," source code for Knox, Samsung's propriety security and management framework present on most of its devices, and confidential data from the U.S. chipmaker Qualcomm, which supplies chips for Samsung smartphones sold in the United States.[19] Access to the breached source could help cyber-criminals find security vulnerabilities that otherwise might not be easily found, potentially opening affected devices or systems to exploitation or data exfiltration.[20]

C. Samsung Suffers a Second Data Breach.

33. Despite the March 2022 data breach, which both exposed Samsung's confidential source code and demonstrated that Samsung's data security measures were woefully inadequate to protect its customers' PII, Samsung continues to fail to implement adequate data security measures.

---

[18] Carly Page, *Samsung Confirms Data Breach After Hackers Leak Internal Source Code*, TechCrunch (Mar. 7, 2022), https://techcrunch.com/2022/03/07/samsung-breach-source-code/.

[19] Page, *supra* note 18; Ionut Ilascu, *Samsung Confirms Hackers Stole Galaxy Devices Source Code*, Bleeping Computer (Mar. 7, 2022), https://www.bleepingcomputer.com/news/security/samsung-confirms-hackers-stole-galaxy-devices-source-code/.

[20] Page, *supra* note 18.

34. Predictably, Samsung suffered another preventable data breach in 2022. However, this time around, the cyber-criminals did not limit their theft to Samsung's own confidential source code. Instead, the cyber-criminals exfiltrated Plaintiff's and Class Members' valuable PII, as entrusted to and stored on Samsung's systems.

35. On September 2, 2022, and just hours before the close of business on a holiday weekend, Samsung announced that an unauthorized third party acquired customer PII from some of Samsung's U.S. systems.[21]

36. Based on Samsung's assertions, the Data Breach began in July 2022, but Samsung did not discover the Data Breach until August 4, 2022 and did not disclose the Data Breach for nearly another month. As such, Samsung knew for weeks that customer PII had been stolen from its systems before it began notifying impacted Samsung users.[22]

37. Given the difficulty of eliminating malware once it has infiltrated a corporate network, especially one as large and complex as Samsung's, the Data Breach is likely a continuation of the March 2022 data breach that Samsung failed to discover.[23]

38. Even if the prior March 2022 data breach and the Data Breach are separate and distinct events, Samsung's repeated data security failures and deficient notice evince a reckless disregard for maintaining adequate data security to protect Plaintiff's and the Class Member's PII from exposure, compromise, and/or exfiltration by cyber-criminals.

39. Samsung's poorly explained Data Breach notice indicates that names, contact and demographic information, dates of birth, and product registration information for certain customers

[21] Data Breach Notice, *supra* note 3.

[22] *Id.*

[23] Allen Bernard, *Impact of Samsung's Most Recent Data Breach Unknown*, TechRepublic (Sept. 9, 2022), https://www.techrepublic.com/article/samsung-data-breach/.

were affected by the Data Breach.[24] Although Samsung's Data Breach notice fails to explain what "demographic information" means, "demographic information" is defined in Samsung's U.S. Privacy Policy as: "technical information about a Samsung user's phone or other device, how they use their device, such as the apps they have installed, websites they visited, ads they interacted with, and precise geolocation data which can be used to identify where a Samsung user goes and who they meet with."[25] As such, it is highly likely that the data now in the hands of cyber criminals reveals detailed information on impacted Samsung users and their online habits.

40. In its Data Breach notice, Samsung further assures its customers that "no immediate action [is] necessary for any of Samsung's platforms," but nevertheless recommends that impacted customers: (1) "[r]emain cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information"; (2) "[a]void clicking on links or downloading attachments from suspicious emails"; and (3) "review [] accounts for suspicious activities."[26]

41. Despite its failure to protect its customers highly personal data, Samsung did not offer impacted customers identity theft protection services. Rather, Samsung merely reminded customers that they are entitled to one free credit report from one of the three major credit reporting agencies.[27]

42. While Samsung has refused to specify the true number of customers who information was affected by the Data Breach, Samsung has hundreds of millions of device users.[28]

---

[24] *Id.*

[25] Whittaker, *supra* note 2.

[26] Data Breach Notice, *supra* note 3.

[27] *Id.*

[28] Whittaker, *supra* note 2.

As such even if the Data Breach only affected one percent of Samsung's customers, the number of people affected by the Data Breach could range from millions to tens of millions Samsung users.[29]

D. Samsung Violated FTC Guidelines.

43. Samsung is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

44. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[30]

45. The FTC provides cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[31]

46. The FTC further recommends that companies maintain PII for no longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

---

[29] *Id.*

[30] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[31] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

on the network; and verify that third-party service providers have implemented reasonable security measures.[32]

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

48. Samsung failed to properly implement basic data security practices. Samsung's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

49. Samsung was at all times fully aware of its obligations to protect the PII of consumers because of its position as a large technology company who collects large swaths of PII from Samsung users. Samsung was also aware of the significant repercussions that would result from its failure to do so.

E. Plaintiff and Class Members Suffered Damages.

50. The ramifications of Samsung's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time.[33]

51. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.[34]

---

[32] *Id.*

[33] Eugene Bekker, *What Are the Odds of Getting Your Identity Stolen?*, IdentityForce (Apr. 15, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics.

[34] *Id.*

52. Besides the monetary damages sustained, consumers may also spend on average over six months and 100-200 hours to discover, resolve, and recover from the effects of identity theft.[35]

53. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

54. Despite all of the publicly available knowledge of the continued compromises of PII, Samsung's approach to maintaining the privacy of PII was reckless, or in the very least, negligent.

55. As a result of Samsung's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certain impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of cyber-criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate an adequate measures to protect the PII that was entrusted to it.

[35] Hari Ravichandran, *How Long It Really Takes to Recover From Identity Theft*, Aura (Oct. 31, 2022), https://www.aura.com/learn/how-long-does-it-take-to-recover-from-identity-theft.

CLASS ALLEGATIONS

56. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the class defined as:

> All individuals in the United States whose PII was compromised in the Samsung Data Breach which was announced on or about September 2, 2022.

57. Excluded from the Class is Defendant, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

58. Plaintiff reserves the right to modify or amend the definition of the proposed Class if necessary, before this Court determines whether certification is appropriate.

59. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective class members through this class action will benefit both the parties and this Court. The exact size of the class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

60. **Commonality.** There is a well-defined community of interest and there are common questions of fact and law affecting members of the Class. The questions of fact and law common to the Class include the following:

a. Whether and to what extend Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII by failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members of the scope of their PII compromised by the Data Breach;

i. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

j. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

61. **Typicality.** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories

and arise from the same failure by Defendant to safeguard PII. Plaintiff and members of the Class were each customers of Samsung, each having their PII obtained by an unauthorized third party.

62. **Adequacy.** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

63. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its common law and statutory duties to secure PII on its systems, then Plaintiffs and each Class Member suffered damages from the exposure of their sensitive personal information in the Data Breach.

64. **Superiority.** The claims of Plaintiff and the Class members are substantially identical as explained above. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members of the Class are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most

manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

65. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

66. Samsung owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing Samsung's security systems to ensure that Plaintiff's and Class Members' PII in Samsung's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

67. Samsung had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by cyber-criminals for unauthorized access, Samsung was obligated to act with reasonable care to protect against these foreseeable threats.

68. Samsung breached the duties owed to Plaintiff and Class Members and thus was negligent. Samsung breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's and Class Members' PII in Samsung's possession had been or was reasonably believed to have been, stolen or compromised.

69. But for Samsung's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

70. As a direct and proximate result of Samsung's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft

protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of cyber-criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Samsung with the mutual understanding that Samsung would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Samsung's possession and is subject to further breaches so long as Samsung fails to undertake appropriate and adequate measures to protected Plaintiff.

71. As a direct and proximate result of Samsung's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiff and the Class)

72. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

73. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Samsung or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Samsung's duty.

74. Samsung violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with the industry standards. Samsung's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach within the technology industry.

75. Samsung's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

76. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

77. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

78. As a direct and proximate result of Samsung's negligence, Plaintiff and Class Members have been injured as described herein and in Paragraph 69 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

79. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

80. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Samsung and that was ultimately stolen in the Data Breach.

81. Samsung was benefitted by the conferral upon it of the PII pertaining to Plaintiff and Class Members and by its ability to retain and use that information. Samsung understood that it was in fact so benefitted.

82. Samsung also understood and appreciated that the PII pertaining to Plaintiff and Class Members was private and confidential and its value depended upon Samsung maintaining the privacy and confidentiality of that PII.

83. But for Samsung's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been entrusted with Samsung. Further, if Samsung had disclosed that its data security measures were inadequate, Samsung would not have been permitted to continue in operation by regulators and participants in the marketplace.

84. As a result of Samsung's wrongful conduct as alleged in this Complaint (including among other things its utter failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that PII), Samsung has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

85. Samsung's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identify thieves.

86. Under the common law doctrine of unjust enrichment, it is inequitable for Samsung to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff and Class Members' PII in an unfair and unconscionable manner. Samsung's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

87. The benefit conferred upon, received, and enjoyed by Samsung was not conferred officiously or gratuitously, and it would be inequitable and unjust for Samsung to retain the benefit.

88. Samsung is therefore liable to Plaintiff and Class Members for restitution in the amount of the benefit conferred on Samsung as a result of its wrongful conduct, including specifically the value to Samsung of the PII that was stolen in the Data Breach and the profits Samsung received from the use of that information.

FOURTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

89. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

90. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

91. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Samsung is currently maintaining data security

measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Samsung's data security measures remain inadequate, despite Samsung's public statement that it took "action to secure the affected systems."[36] Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

92. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Samsung owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. Samsung continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

93. This Court also should issue corresponding prospective injunctive relief requiring Samsung to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

94. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Samsung. The risk of another such breach is real, immediate, and substantial. If another breach at Samsung occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

95. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Samsung if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft

[36] Data Breach Notice, *supra* note 3.

and other damage. On the other hand, the cost to Samsung of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Samsung has a pre-existing legal obligation to employ such measures.

96. Issuance of the requested injunction will not disserve the public interest. To the contrast, such an injunction would benefit the public by preventing another data breach at Samsung, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and,

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: November 23, 2022

/s/ Gary F. Lynch
Gary F. Lynch
Jamisen A. Etzel
Nicholas A. Colella
Patrick D. Donathen
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: 412.322.9243
Facsimile: 412.231.0246
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com
patrick@lcllp.com

(Eddie) Jae K. Kim (*pro hac vice* forthcoming)
LYNCH CARPENTER, LLP
117 East Colorado Blvd., Suite 600
Pasadena, CA 91105
T: (626) 550-1250
ekim@lcllp.com

Attorneys for Plaintiff